2021-01-29

A Conceptual Cyber-Risk Assessment of Port Infastructure

Tam, Kimberly

2021 World of Shipping Portugal. An International Research Conference on Maritime Affairs
28-29 January 2021, Virtual Conference, Parede, Portugal (Accepted Manuscript)

A CONCEPTUAL CYBER-RISK ASSESSMENT OF PORT INFRASTRUCTURE

Tam, Kimberly. University of Plymouth, PL4 8AA, UK, Kimberly.tam@plymouth.ac.uk
Moara-Nkwe, Kemedi. University of Plymouth, PL4 8AA, UK, kemedi.moara-nkwe@plymouth.ac.uk
Jones, Kevin D. University of Plymouth, PL4 8AA, UK, kevin.jones@plymouth.ac.uk

ABSTRACT

Cyber-security is a growing issue across the world, however increasing concerns are being directed at ports, as they are a hub for multiple transport operations. Ransomware has shown its potential effects in recent events, infecting logistic infrastructure at Maersk and United States of America oil pipelines. As a part of a European Union Project called Cyber-MAR, researchers have been given data from several ports on the cyber-environment of their facilities. The main goal is to raise awareness of cyber-risks in ports and potential mitigations with the novel application of a dynamic risk assessment tool (Maritime Cyber Risk Assessment or MaCRA) to ports. MaCRA methodology uses a dynamic risk model to analyse maritime risks specifically, as cyber-attacks on ships and at the ports can have hard implications in both the cyber and real world. This paper uses generalised port data to create a preliminary, conceptual cyber risk assessment of ports, to raise awareness by building general risk profiles without revealing real port vulnerabilities. From this risk assessment, the authors expect to find several high-level cyber-risks that ports may need to address, as well as some scenarios that could increase or decrease those risks. The limitation of this research is the availability of data, which is somewhat mitigated by Cyber-MAR port partners. The main goal is to raise awareness of cyber-risks in ports and potential mitigation measures with the novel application of a dynamic risk assessment tool (MaCRA) to ports. This also provides a basis for further research in Cyber-MAR, as the authors will be using simulation and more real-world data to enhance the findings in this conceptual paper.

Keywords: Maritime, Risk, Port, Cyber-security, Cyber-MAR

1. INTRODUCTION

Similar to other critical infrastructure globally, a nation's ports face an evolving number of cyber threats. The port infrastructure and services are highly diversified, with ports adapting their infrastructure and services to local geographic, territorial, and customer specificities (ENISA, 2019). The maritime sector handles 90% of the world's goods, most of which passes through ports, with the volume reaching 11 billion tonnes in 2018 (International Chamber of Shipping, 2019). Not only is the need for efficiency increasing, but more often, both ships and ports are expected to be more environmentally friendly and strategically sustainable. The global shift of activities and measurements to achieve high standards of efficiency and sustainably are developing new capabilities promoting new technologies (e.g. remote control, digital twins, automation). However, while this creates useful technology solutions, they may also increase the risk of cyber-related incidents, whether by accident or an attack. The maritime sector has begun incorporating solutions like the Internet-of-Things (IoT) to computerise information, gather information in large quantities, and increase communications, whether remotely, locally, machine-to-machine, or human-to-machine. Superficially in the maritime sector, the IoT revolution has also sped-up the convergence of information technology (IT) and operational technology (OT), bringing a new generation of smart ports (Yang, et al., 2018), or sometimes known as 'Ports 4.0' as a reference to the industry 4.0 era concept (Lasi, Fettke, Kember, Feld, & Hoffmann, 2014). The pressure for efficiency (e.g., time, cost) has also accelerated the adoption of autonomous solutions, fully, semi-autonomous, and remote access, in both ships and ports (PortForward, 2018) (Akbar, et al., 2020).

As this paper was written within the scope of the Cyber-MAR project[1], the remainder of this article will tend to be biased with its usage of European statistics. This is still significant, as European ports have handled an estimated 3.6 billion tonnes in 2018 (Europa, 2020). Although several findings will be high-level and conceptual, because of the nature of the project, there will be limitations based on the availability of real port information. Therefore, the authors will attempt to indicate when generalised findings are more likely appropriate to European regions of interest, as opposed to world-wide risks. In the project's context, this paper looks at two pilot scenarios defined by the port partners: (1) $Pilot_1$ cyber-attack resulting in a power outage, and (2) $Pilot_2$, disruption to flow of container to rail through a cyber-attack on port cranes. More details on good practices for ports and overall port services, infrastructure, and systems can be found in documents for, namely (ENISA, 2019). This paper aims to examine ports using generalised data from two concrete scenarios, to create a conceptual cyber risk assessment of ports focusing on abstracting higher-level concepts. While this yielded interesting findings, additional assessments of future ports will be made by considering maritime technology trends, as both port and ship technologies become more complex, integrated, and ubiquitous. Currently, when looking at the today's ports, it is difficult to find a plausible attack that could disrupt a port on the order of weeks or months, as opposed to hours. While there will be some discussion around future issues, the focus is still not on complex ports (e.g. fully autonomous), or those specialised for other services (e.g. dry bulk), which present different risk profiles relative to the ports involved in Cyber-MAR; while there will be overlaps, differences will be more pronounced.

The remainder of this paper is as follows: Section 2 provides a relevant background of IoT, IT/OT, and power in the maritime sector. Section 3 builds on this by discussing these elements in the context of Cyber-MAR's cyber-security pilot scenarios. This is done by extracting data from the main project and assessing cyber-risks and vulnerabilities to generalise, and abstract. Section 4 is dedicated to the more concrete MaCRA (Tam & Jones, 2019b) risk profiles generated as a part of the project, while Sections 5-6 concludes with the more high-level and conceptual aspects to continue risk discussions into both more general ports security as well as future, smart port security.

2. BACKGROUND

The area of maritime cybersecurity is relatively new and combines well established maritime safety with the newer challenges of cybersecurity, an area that, in comparison, is volatile and evolving rapidly. Maritime-cyber security, therefore, focuses on how technology affects new and traditional concepts of safety at sea and at port. In order to discuss the pilot scenarios, which were pre-defined to target power and cranes, it is necessary first to examine the relevant cybersecurity and maritime elements in detail. Specifically, it is important to discuss details around the IoT, IT/OT, power, and communication in a port setting. A high level of port infrastructure and services can be found in (ENISA, 2019), although this is not designed to represent specific ports, as most ports will not provide all possible services listed and instead specialise in a subset of those services (e.g. oil, passenger).

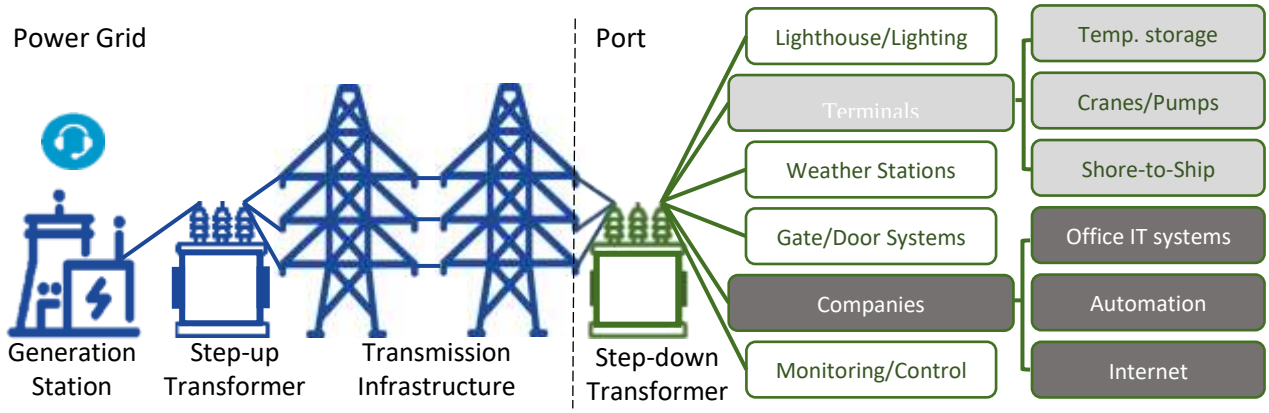
Of the top 20 European cargo ports handling containers in 2020, the most specialised were Bremerhaven, Piraeus and Valencia (Europa, 2020). In contrast, those most specialised ports handling liquid bulk were Botas and Bergen, therefore, any individual port risk analysis would not represent overall or general risks. In addition to seeing a port from a single high-level view, ports can be divided into several layers to fully explore the cyber, cyber-physical, and physical elements (Polemi, Ntouskas, Theoharidou, & Gritzalis, 2013) (Tam, Moara-Nkwe, & Jones, 2020). This deviates from most cyber-security risk assessments, where air-gaps are considered as relatively secure, whereas cyber-physical attacks could affect several 'layers', propagating attacks in novel ways.

[1] Cyber-MAR: https://www.cyber-mar.eu/

2.1. Power

The cyber-security issues of smart-grids has a significant body of research dedicated to it, as power has long been considered critical national infrastructure (Khurana, Hadley, Lu, & Fincke, 2010) (Tan, De, Song, Yang, & Das, 2017). While an attack on the wider power grid would result in a port losing power, which satisfies the first scenario, which the authors called $Pilot_1$ in Cyber-MAR and Section 1 and detail further in this section, this is not a port-specific attack and therefore less interesting when assessing port risks. Instead, this paper will be focusing on the less explored attack scenario where the port is specifically targeted. This scenario defines the separation between the larger national grid infrastructure and 'the port' at the local step down transformer(s), as shown in Figure 1.

Figure 1: Port power and power grid definitions for port scenario 1.



Source: authors own elaboration

In addition, Figure 1 generalises several key port components that rely often rely on power. This was abstracted from the information provided by ports for the Cyber-MAR pilots described in Section 3 of this paper. It is important to note there are many other systems (e.g. lighting, safety systems, passenger facilities, temporary storage) that could be considered. According to a study of more than 90 European regions and cities, in 2017, it was estimated that typical power distributions at a terminal account roughly 40% for refrigerated containers waiting in temporary storage, 40% for ship-to-shore container (STS) cranes, 15% to yard lighting and 5% to offices (FCH, 2017). Later in Section 3 of this paper, all these systems are considered by the authors to be critical to core port operations. However, much of the risk assessment being performed will focus on the ones that are most likely to cause significant delays if they are shut down due to lack of power.

Besides the endpoints for power, transformers are also critical port components. Considering cyber-physical risks, environmental challenges have also affected transformer builds (e.g. liquid vs dry) which, if physically damaged, can affect the repair time in Section 3 scenarios (Brown, 2017) (Edris & Hoidalen, 2012). Not only do step-up and step-down transformers make long-distance electric power transmission practical, making the 'port' step-down transformer a point of potential attacker interest, other port power vulnerabilities are the transformers placed across the terminals to power various services. Besides the refrigerated containers mentioned previously (i.e. reefers), something uniquely relatively to port power are the transformer kiosks that can provide power to ships. The physical gap is often closed with smaller cranes to connect shore cables to the ship.

Due to for environmental reasons and regional differences these kiosks may need to supply different voltages, for example, 1,5 MVA for Ro/Ro and 15 MVA for cruise ships (Peng, et al., 2019). In Figure 1, these shore-to-ship converters are considered a part of a terminal, and a port may have

several terminals designated to certain services (e.g., container cargo versus cruise passenger). Therefore, services from pumps and cranes are also critical for operations at those terminals. In addition, while some cranes like rail-mounted gantry cranes (RMG) are fully electrified, others like rubber tyre gantry cranes (RTG) which are more often powered by diesel generators due to their mobile nature. The following sections will further detail the cyber and cyber-physical risks to these unique port systems and services. Power infrastructure often use redundancies like back-up generators to ensure constant power, and in Section 3.2 we discuss how difficult this may be. However, to follow the terms of the project and explore the possibilities makes this scenario an interesting case.

2.2. Port Communication

Another critical part of port infrastructure is the communication channels to allow machine-to-machine, human-to-machine, and human-to-human connections. In a port, and from ship-to-shore, several technologies are used from radio, Wi-Fi, satellite (e.g. 3G, 4G, 5G), and telecom (Polemi N. , 2017). Each of these has a body of work examining the cybersecurity issues, with Internet and satellite protocols receiving the most recent attention (Brogaonkar, Hirschi, Park, & Shaik, 2019). That said technologies, such as radio-based identification, are commonplace in ports whereas they may be less popular in other environments. For example, radio frequency identification (RFID) are commonly used in logistics, container identification, and cargo management, but have known vulnerabilities, such as physical attacks to alter or copy data, denial or service, and brute force attacks to read data (Jain, Chaudhary, & Kumar, 2018). Port communication technology and the data that gets transferred are critical for a series of services. Therefore, the connectivity between systems, as well as interfaces for users, means that security is a growing concern. Due to the pilot specifics, for the power scenario ($Pilot_1$), the only cyber-attack of interest is a denial of services (DoS) attack as that would result in a power outage. While power grids do face issues with theft and false meter readings issues, that is not the focus. In comparison, in the second pilot scenario must consider a wider selection of cyber-attack categories due to its setup.

In contrast, $Pilot_2$ examines attacks that would result in loss of control of a gantry crane, affecting the movement of containers within port terminals. Due to this, the attacks of interest are cyber and cyber-physical actions that are DoS and/or hijacking in nature. In the $Pilot_2$ scenario, the communication technology of interest concern cranes, primarily those that enable remote access and control, but also remote monitoring. A maritime port usually has two main classes of cranes, quayside cranes such as STS cranes and yard cranes such as RMG cranes. The efficient operation of both these cranes is usually dependent on a variety of supporting IT/OT infrastructure, including communication channels and protocols. The smooth and timely implementation of STS unloading operation can, therefore, be dependent on multiple supporting systems and processes to operating efficiently. This includes the availability of VHF radio which is used for both ship-to-shore communications and intra-port communications. The unloading operation is conducted with the help of an unloading plan, which outlines which containers are to be unloaded for import, and the location of those containers within a container ship's hold. This is normally achieved with the unloading plan, which particular for container ships, are created between the ship and terminal. The bay plan, which indicates were the containers are, is performed at the loading port and is also affected the sequence of the vessel ports of call. This may be different for dThe procedure for storing and distributing this information should be assessed to determine security risks.

The reverse of the STS unloading operation is STS loading, which is also conducted through a wide suite of IT/OT systems, particularly communication systems. This includes the not only the crane itself but the IT systems that usually host both the terminal operating system (TOS) that perform critical stowage planning operations and the databases that store port and vessel information. The stowage plan is communicated to all involved parties involved with loading operations to ensure containers are loaded into local port storage in the right order. If the IT systems hosting TOS have

network interfaces for external connections to them (e.g. Internet access), then work needs to be done to assess the risks that arise from that. Furthermore, the assessment must be made of the expected impact on port operations, e.g. the potential loss in access or availability of such systems due to a cyber-attack. The loss of access to these systems in a port will cause a reduction in the capabilities at the port terminal, which will lead to lower effectiveness and, consequently, lower container throughput of the port. The lower effectiveness of port operations can then lead to delays in container processing which would propagate through the supply chain and cause delays further down, for example, with rail. Modern wireless remote controlled cranes pose additional advantages over traditional cranes from an efficiency viewpoint, but also pose additional cyber risks to port operations. Current technologies that supply wireless access tend to use 3G/4G at port terminals, but wireless is sometimes also offered (Bo & Wang, 2019). Furthermore, as existing regulations, standards, and risk management are not currently adequate to address today's maritime-cyber port threats today, it is important to examine future, smarter, ports as well (Polemi, Ntouskas, Theoharidou, & Gritzalis, 2013), which Section 5 covers.

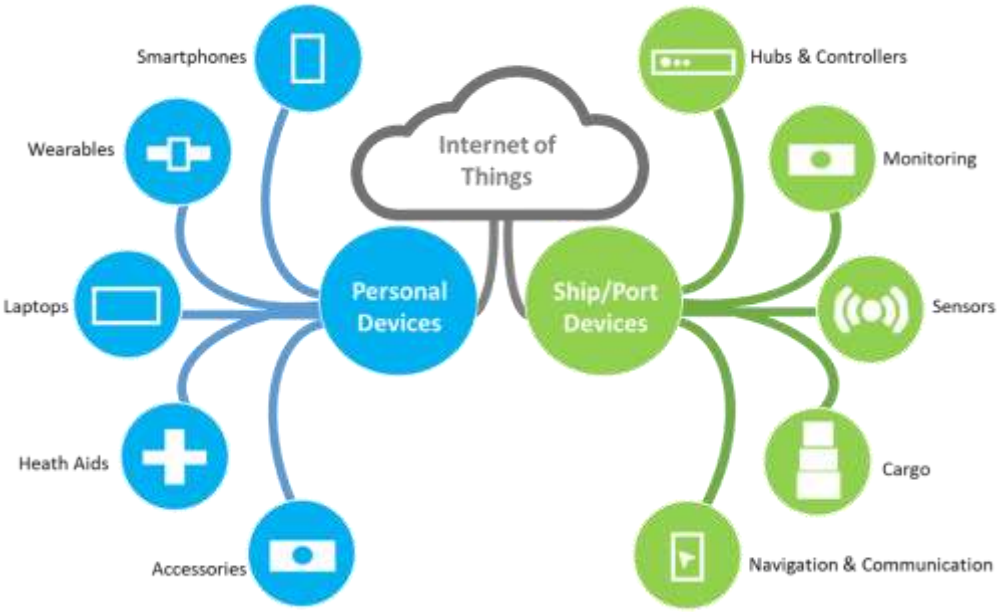
2.3. IoT and IT/OT Convergence

On top of the port of infrastructure, which uses a combination of Internet and other communications for maritime operations (DNV GL, 2015), there are also all the devices from workers and passengers to consider. Therefore, the port IoT concept includes many types of interconnected devices belonging to both the port services and users. In a survey carried out, the outcome shows that 42% of maritime organisations believed that they could benefit from additional IoT skills and 2.3 million Euros might be spent on IoT solutions between 2018 and 2021, more than on big data analytics or cloud solutions (Brandy, 2018). Furthermore, with the COVID pandemic in 2020 highlighting some supply chain concerns, we may see further investments in IoT solutions regarding supply chain and logistics issues. With the addition of possibly more workers working remotely increases both the chances of an attacker infiltrating a system, and the decreases the chances of being detected by people. As IoT is a broad definition, many devices will be included in such networks; however, as discussed in Section 2.2, not all port communications use Internet protocols. Therefore, port IoT could be considered a subset of the wider port communication network, and only one layer of infrastructure.

Considering maritime IoT devices, these can be categorised broadly into personal devices, ship devices, and port devices (e.g., power grid sensors, crane controllers). As seen in Figure 2, personal and maritime-specific devices are separated as the first takes common technology and injects them into a maritime context. In contrast, ship/port devices are unique even though parts of the underlying technology can be considered commonplace. Besides, as IT and OT converge across both ships and ports (Man, Lundh, & MacKinnon, 2018) (Ray, Harnoor, & Hentea, 2010) the communication layer will intersect more with others. In particular, sensors are likely to become the most common form of IT/OT convergence as a net of sensors is a good solution for gathering information for determining efficiency and environmentally friendliness in power, cargo management, and more.

As the industry moves towards the future, modern ships may increase on-board devices to over 8,000 data tags and sensors for monitoring and control. With IoT growth in the sector, it has also been reported that 87% of mariners think that IoT security can be improved (Brandy, 2018). As containers are also often electronically tagged and port infrastructure evolves, a significant portion of a future global IoT could be dedicated to maritime operations. Autonomous, semi-autonomous ports such as Rotterdam (Martin-Soberon, Monfort, Sapina, Monterde, & Calduch), and smart ports blending with smart cities like in Belfast (Belfast Harbour, 2019), will likely push ports to converge IT/OT further and seek increased monitoring, fine-grained control, remote access, and autonomy. This will likely increase port communication in general, at the expense of a significant increase in IoT solutions.

Figure 2: Maritime IoT in addition, and integrated, with existing infrastructure.



Source: authors own elaboration

3. PORT CYBER-SECURITY PILOTS

This section considers the two pilots designed around the port partners of the Cyber-MAR project. In particular, it will discuss how the two hypothesised port cyber-attacks scenarios could play out in detail. However, instead of using the specifics of the two ports identified by the project (i.e., the port of Valencia and the port of Piraeus) this paper will generalise figures and findings to provide a more general, high-level, cyber risk assessment. While details will be altered, some will be purposefully altered or obfuscated to protect individual port vulnerabilities while illustrating the overall concerns and risks explored as a part of this project. With the context of the pilots and the proposed sequenced cyber-attack chains, Section 4 discusses the MaCRA findings for project Cyber-MAR as well as the more generalised findings of this paper extrapolating from was learned. In addition to the current project findings, this paper considers further complications that may be found in the next generation of ports (i.e. port 4.0, smart ports), that use autonomous or semi-autonomous solutions in Section 5.

3.1. CYBER-MAR

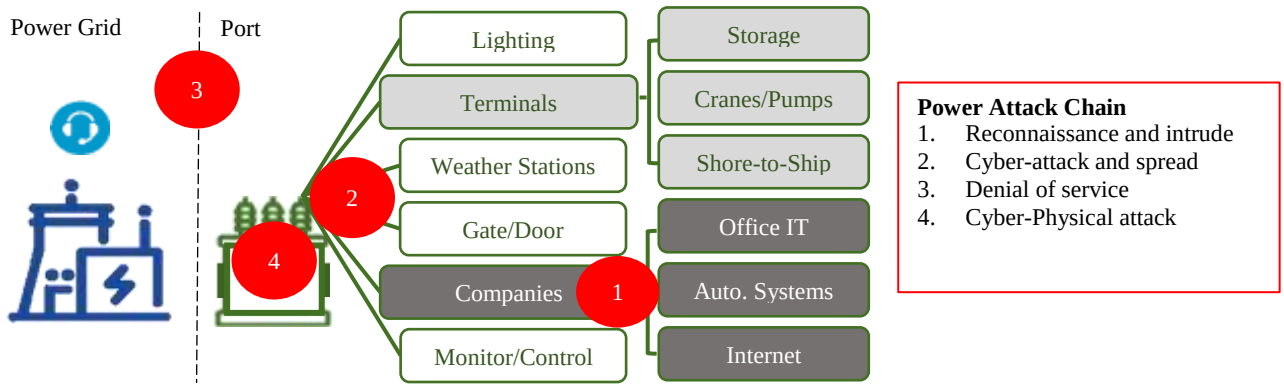
The primary purpose of the Cyber-MAR project is to develop innovative simulation environments that accommodate the unique peculiarities of cybersecurity in the maritime sector. In order to meet this end, several intermediate steps were defined, and one of those was assessing three pilot scenarios. Two of these discussed port-side concerns and issues, while the third addressed vessel navigation and on-board autonomous systems. The purpose of this paper is to examine the first two-port scenarios and extrapolate to more general findings, as seen in Sections 3.1 and 3.3. However, it is important to note the limitation of the data provided. Although the two pilots are different, they by no means represent the majority of port services and environments of ports globally. For example, as two Mediterranean ports, this study is unlikely to fully understand the cyber-physical risks associated with ports with low visibility, extreme tidal differences, and extreme temperatures. However, in 2018, 11 of the 20 top cargo ports in Europe were located in the Mediterranean (Europa, 2020), so general findings should still be relevant to the European Union (EU). Furthermore, both Piraeus and Valencia belong to the top 20 specialised ports for containers (Europa, 2020); therefore, they will have very

different infrastructure and services compared to other ports, such as Bergen and Botas which are more specialised in the crude oil sector. Section 4 and 5 will explore these differences further, and the effects on risk, when considering ports in geographical location as well as ports that do not fit the specialised container port profile.

3.2. Power outage

The first port scenario considers an attack scenario (i.e. an assault launched using one or more computing devices against one or more devices or network of devices locally or remotely), targeting the energy management system of a port. The outcome of such an attack would affect operations and relevant parts of the local electrical grid. The main objective of this attack is to cut off the power supply to port infrastructure and services and avoid triggering emergency power systems, increasing the outage duration. This will firstly cause a denial of service effect, however, if the outage lasts long enough it is possible to cause damage, particularly to equipment designed to be in motion constantly and the storage of goods. Consequently, it is important to address the feasibility of an attack that could cause such an outcome. To do this, the authors examined past cyber-attacks in similar environments that can be applied. These are not direct copies of the other attack sequences, but conceptual adaptations appropriate for port environments. More importantly, in this scenario, the authors detail the cyber-attack, targeting port power, as an attack chain. This attack chain, again based on real cyber-attacks of the recent past, aims to show that there are different levels of severity. In Pilot$_1$, the severity is gauged by the loss of time, and the delay to operations as the paper is interested in the econometric results (e.g., loss), based on the time delay, brought on by a port cyber-incident such as this.

Figure 3: Power attack chain sequence of a port in the Pilot$_1$ scenario.



Source: authors own elaboration

The primary inspiration for this attack chain, to achieve a port power outage, was the 2015 cyber-attack on the Ukraine power grid (Lee, Assante, & Conway, 2016). As explained in Section 2, while an attack on the generating station, generator step-up transformer, transmission lines or customers would have the same power outage outcome in the port, this paper considers those as attacks on grid infrastructure, instead of an attack on port infrastructure. To comply with the aims of the project, the authors exclude "grid" infrastructure and instead consider the local substation step-down transformer, port sub-transmission components (Brown, 2017), and other local port components as a part of the port. Therefore, due to the definitions of the pilot, the authors were primarily interested in attacks that target these components. Conceptually derived from the Ukraine attack, the authors propose the following attack chain to cause a similar denial of power in a port environment. This is illustrated in Figure 3 and detailed in the following subsections.

3.2.1. Reconnaissance attack

Power infrastructure has evolved much in recent history, with several protections and redundancies to provide constant power in most nations. Therefore, it is highly unlikely that an accidental cyber-event could shut off both main and back-up power will at a port, however, this does not mean that unintentional cyber-attacks cannot have severe outcomes (Maersk, 2017). Intentional attacks (i.e. cyber, physical, cyber-physical) strongly deviate from random failures, something that has been examined for both general IT but also OT such as power (Sole, Rosas-Casals, & Valverde, 2008). Therefore, for an attack-chain sophisticated enough to achieve significant power outage outcomes, reconnaissance attacks are likely needed to gain critical knowledge of a target. This would likely include unique aspects of the target, in this case, transformers and SCADA networks, common to OT and infrastructure (O'Flaherty, 2020) (Safa, Souran, Ghasempour, & Khazee, 2016) (Rockwell Collins, 2017)(BBC, 2011). As seen by past studies, OT is also known to be vulnerable, even though much of the global focus is on IT cyber-security. As SCADA networks and other OT components are often highly specialised to services provided, reconnaissance, either remotely or locally (e.g. insider threat) is likely needed for an attacker whether by an insider or outsider attacker. The origin would likely mostly determine the time needed to gather information, and the level of detail.

In this paper's attack chain, a combination of social engineering and information gathering actions is used to understand topology vulnerabilities and attack vectors within the port system, focusing using business IT for the initial attack but then power OT (e.g. transformers and SCADA connectors) to increase damage and duration. This can be done with internal or external human attackers, even in maritime (Tam & Jones, 2019b). As a first step, reconnaissance does little to no damage and often seems like legitimate behaviours, making it very difficult to detect and sometimes to mitigate. In the Ukraine example, reconnaissance was done with external spear-phishing; however, a disgruntled or temporary employee could achieve the same level of information gathering. Without proper security, insider threats cannot only execute attacks but also open back doors for other attackers.

3.2.2. IT cyber attack

With the successful gain of target information, the next step in this paper's attack chain for $Pilot_1$ to cause port blackouts is to execute cyber-attacks that target business IT which, during reconnaissance, was found to be vulnerably connected to other port systems. Considering the Ukraine attack, this is not impossible, just unlikely if appropriate office security solutions were implemented. However, with the availability of crafted malware and IT attacks sequences or chains, an attacker can also rely on existing hacker resources like black-markets (i.e. dark web) to make this initial penetration easier (Thomas, et al., 2017). Stolen credentials bought on the dark web or stolen directly during step one can also greatly aid an IT attack or even hide indicators of cyber-attack. Both classic IT attacks were employed in the Ukraine power attacks (Lee, Assante, & Conway, 2016), when boot records and logs were deleted, and stolen credentials were used to access the relevant power grid systems remotely.

While IT cyber-attacks may change in the future, adapting to fully autonomous or otherwise smart ports, currently, the main vectors of attack likely start with traditional IT systems, as they are often more connected to wider networks, are used by more people, and have more known vulnerabilities known, and exploited, by the hacker community. That said, as discussed in Section 3.2, attacks to OT, even air-gapped ones, are possible. However, based on current events, IT attack vectors are the most plausible and therefore, the focus in this power outage pilot. In the port power outage attack sequence, the cyber-attack can be further broken down into malware installation to switch substations off and disabling IT infrastructure to cause further delays by hindering defence and mitigation efforts to reverse outage effects. Unlike Reconnaissance attacks, which can be difficult to detect because they are the closest to normal and legitimate behaviours, the profiles of malware attacks are often

more easily recognisable, and security solutions such as intrusion detection systems (IDS) can be implemented to deter this set of the larger attack chain. This will be further discussed in Section 5.

3.2.3. Denial of Service Attack

As seen in part three of Figure 3, a denial-of-service (DoS) attack can prevent the target from receiving help during an attack. That is what happened in the Ukraine, power infrastructure focused, attack, as some fake calls were used to preoccupy power grid helplines and to decrease the likelihood of legitimate power-outage reports from gaining attention. However, remotely targeting the call centre of the energy company is not the only way a DoS attack can be made. The Ukraine attack approach is highly applicable to a remote attacker. However, an insider threat, especially one who has acquired knowledge and credentials they should not have during a reconnaissance attack, could more easily stop calls for assistance at the source. This is much more sophisticated, targeting specific people, systems, or communication channels, and has a higher chance of success as it does not negatively affect players outside the targeted port area. Therefore, by deviating slightly from the established Ukraine power-grid attack, in this conceptual port power cyber-physical attack, the authors assume that more sophisticated denial of service attacks were used to stop calls for assistance, prolonging the power outage by a few hours.

A power outage by its nature is a DoS attack, denying power to infrastructure and services as its primary outcome. However, for some systems, a long period without power could cause secondary effects like damage. For example, patients in hospitals can lose their lives during a significant power outage (Klinger, Landeg, & Murray, 2014). Within a port, particularly ones specialised to cargo, the systems of concern during a long power outage would be the ones related to cargo storage and maintenance. For example, refrigerated containers, reefers, can use up to 40% of a terminals power (FCH, 2017) (Duin, Geerlings, Tavasszy, & Bank, 2019), and without power, contents may spoil if unpowered for hours, depending on cargo and environment. That said, mitigating damage may be relatively easy, as reefers are mobile by design and can run off generators, but usually only for about 24 hours when marine insurance cover often is triggered to start. For later stages of the Cyber-MAR project, focusing on the econometric effects instead cyber risks, this will be critical in understanding the econometric losses by nation, and by industry, of which frozen meats and pharmaceutical may be affected with reefers affected. This is included in discussions about future work. Ships can also use shore-side electricity for recharging, for greener purposes (Dai, Hu, & Wang, 2020), however again it is not needed, and generators can be used. Reduced lighting and office (15 - 5% respectively) could also increase the chance of accidents (e.g., at night) and further reduce to port operations.

3.2.4. OT Cyber-Physical Attack

In 2018, ships spent a median time of 23.5 hours at port (International Chamber of Shipping, 2019). Less time spent at port often indicates a higher level of efficiency, and to continue the trend of efficiency ports are often turning to technology to provide more information, control, and automation. Greener energy has also driven ships to be more efficient, encouraging more monitors and sensors, and to draw more power from ports when available. In the Ukraine attack chain, it eventually targeted uninterruptable power supply (USP) systems to trigger a scheduled service outage at a time convenient to the attacker. While this had the physical outcome desired, a power outage, it was fixed fairly quickly because it was purely a cyber-attack. However, analysers of the Ukraine attack (Lee, Assante, & Conway, 2016) worry that attackers could have used their acquired control and permissions to cause physical damage to the power infrastructure, and possibly surrounding areas if fires are started, and prolong power outages. The fear is that instead of, or in addition to, the malware used in the Ukraine attack, more sophisticated malware, nearer to the level of Stuxnet (Chen & Abu-

Nimeh, 2011) could cause physical damage to power infrastructure, such as the transformers. It is important to note that an attack like that has not been fully realised in either real ports or power infrastructure, however many studies highlight valid concerns moving forwards.

The main realisation of Stuxnet, which targeted industrial control systems and caused physical damage, is that targeted cyber-attacks can cause significant physical damage, even threatening lives. With the convergence of IT and OT, more sensors are being added to power infrastructure to monitor control electricity usage. This is supported by the drive to be greener and more efficient but introduces new vectors of vulnerability (Chen & Abu-Nimeh, 2011). With more power options than 'off' or 'on' in future scenarios, then there is an increased risk of misinformation. With misinformation, the manipulation of power through cyber-attack can be more complex. For example, lowering the power outages by exploiting a UPS, but not completely shut it off, or hacking monitoring sensors to prevent systems from reporting drops in power, are ways to misdirect and obfuscate an attack further. The issues can be exasperated if there are no back up sensors for resiliency. Damaging a transformer could also delay power denials. For example, compromised sensors could allow a transformer to overheat. This may be even more relevant in semi-autonomous or fully autonomous ports or otherwise smart ports with highly integrated IT/OT. Some estimates for repairing a damaged transformer is roughly two to five days, with replacing larger ones at one to two months (Brown, 2017) (Adoghe, Awosope, & Ekeh, 2012) (Foster, et al., 2008), which could significantly prolong the cyber-attack induced power outage, as in the Ukraine example, which reported outages of up to six hours.

The actual time for repair for a port could vary significantly, as repair time relies heavily on the transformer type and how quickly repairs or replacements can be brought on site. That said, damaging a transformer does not guarantee a noticeable power outage. As an example, one without a cyber-attack element, a sniper attack in 2013 severely damaged 17 transformers in a transmission substation. While it took 27 days and 15 million USD to repair, blackouts were averted by re-routing power (Bi, Zhang, Wang, & Ding, 2019). If prepared, a port could likely avert a cyber-physical attack on power infrastructure. However, without appropriate security and mitigation strategies, especially if moving towards smart or semi-autonomous ports, it is possible an enhance and targeted attack chain, similar to the one used in Ukraine, could cause a power outage on the magnitude of days instead of hours.

Besides a potential denial of service to lighting, which, as explained earlier, could increase the risk of accidents in the right conditions, gates, doors, and other locking mechanisms can affect cyber-physical risks. This is likely a lower concern than others, however, depending on whether electronically locked gates and doors fail open or fail closed, this could slightly increase the risk of theft or physical intrusion as another form of cyber-physical attack. Furthermore, if a port includes dock gates or similar (Allianz, 2014), this could increase cyber-physical risks further if triggered with an attack, instead of a failure (Crouigneau, Bourdon, Billard, Person, & Schoefs, 2008). Lastly, similar to the loss of lighting during a power outage, ports may also be denied safety systems, such as fire repressing systems. This becomes increasingly problematic when considering ports that handle difficult or hazardous materials such as oil (Kosmowski & Gotebiewski, 2019). Therefore, the outcome of this step in the attack chain will have the most varying outcomes based on the port itself.

3.3. Wireless attack

As the container shipping segment continues to consolidate in recent years, the combined market share of the top ten container shipping less was 90% in 2019. However, this was a 22% increase since 2014 (International Chamber of Shipping, 2019). European port traffic has also increased 4.7% from 2017 and, as of 2018, had 16% of global container port traffic, second to Asia with 64%. In Europe, eleven of the top twenty cargo ports in 2018 were located in the Mediterranean (Europa, 2020). Because of this, and because ports analysed by Cyber-MAR, some of the environmental elements align more with $Pilot_2$ settings.

In the second pilot scenario, instead of a denial of service on power, it examines a wireless cyber-attack on a port's gantry crane control systems, causing delays or damage. In $Pilot_2$, this scenario is specifically for examining cascade effects of container movement delays port to the inland. To better simulate a port's operational levels, the authors created a representative port using relevant container operational systems using (Simul8, 2020), and as seen in Figure 4. As can be seen, $Pilot_2$ focuses more on the terminals that deal with container ships and ship-to-rail crane operations. In order to achieve the many operations required at a container terminal and beyond, a port will often have several different cranes for operations with different risk profiles determined by the services they provide (i.e. popular devices are often targeted more) or by the ease of the attack (i.e. some cranes may be easier to attack remotely, through remote monitoring or control for example). For Cyber-MAR one specific port is being analysed; however, the authors have generalised and created a conceptually similar port in Figure 4. Specifics on types of cranes, crane details, and the number of cranes has been altered. Similar to the previous conceptual $Pilot_1$, to increase the realism of the attack, despite removing some port-specific details, relevant research on security analysis of industrial robot controllers, or industry 4.0 technologies, will be used to understand better and assess the possible cyber-physical threats of wirelessly connected port cranes.

Figure 4: Example port container operations generated with Simul8.

Figure 4.1a: Overview of Port Processes

Figure 4.1b: Incoming Container Processing

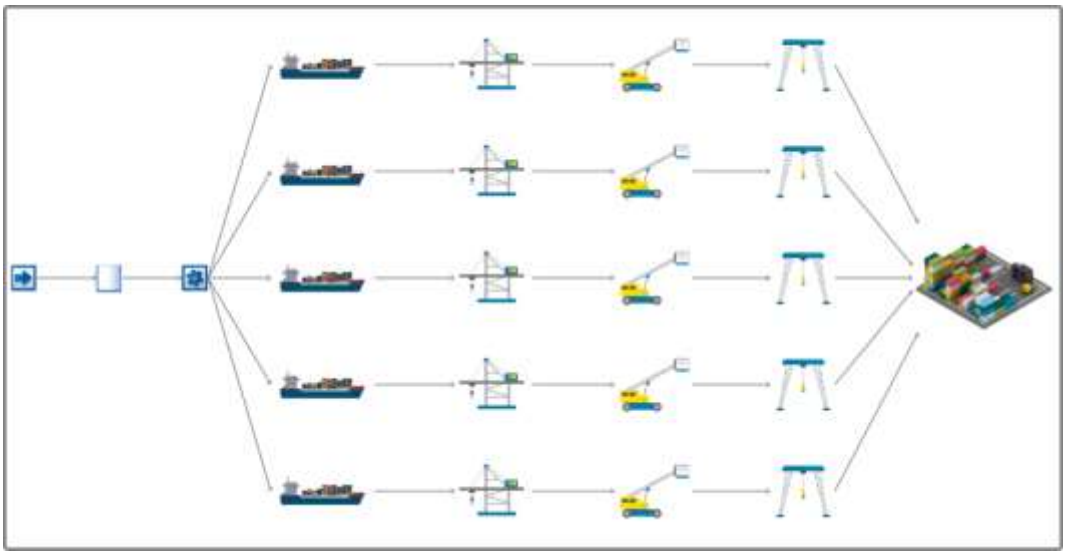
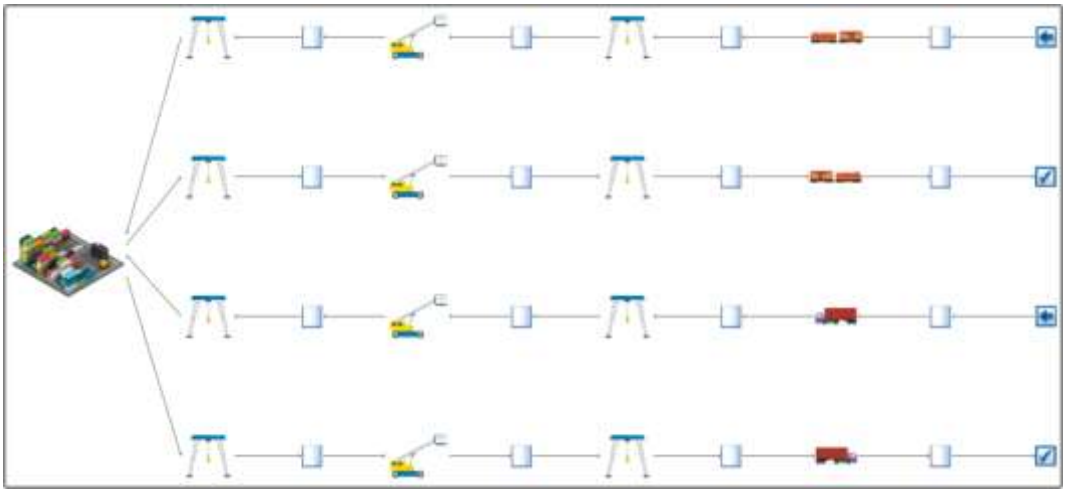


Figure 4.1c: Outgoing Container Processing



Source: authors own elaboration

Cranes are used for a wide range of operations; however, the focus in this paper are ship-to-shore (STS cranes), or cranes that primarily handle cargo containers. As mentioned, these can consume up to 40% of a port's power, representing a large draw and a significant part of port operations. That said, mobile cranes, often referred to as rubber tyre gantry cranes (RTGs), are also critical for moving cargo to rail and road vehicles, and are not directly reliant on port electricity but primarily generators or batteries in electric eRTGs (Antonio, et al., 2016). The port of Valencia is reported to have eighteen eRTGs and seven dRTGs, while Piraeus is reported to have 30 eRTGs. In order to cause significant disruptions to crane operations, $Pilot_2$ looks at several types of attack including denial of service and control hijacking, as these can all prevent legitimate crane operations from being completed either by damaging the equipment or through communication obfuscation and manipulation. Furthermore, in addition to Cyber-MAR objectives, instead of only examining the loss of control the authors will also examine the risks and effects loss of monitoring or the manipulation of monitoring systems in the context of next-generation smart ports and autonomous systems in Sections 3.2.1.-3.2.3.

3.3.1. Cargo movement

While the average size of vessels calling at large European ports has been trending up for last 15 years, from 2017 to 2018, it decreased by 3% to almost an average of 7,383 GT in 2018 (Europa, 2020) and it possible that this has slowed down further due to the 2020 pandemic. That said, the average size of container ships, specifically, has pushed the evolution of cranes, physically and in control technologies, in addition to the pressure to increase efficiency. This scenario looks primarily at wireless vulnerabilities in current crane technology but also considers relevant industrial cyber-physical security as there may be similarities in the technology used and operational flows.

As seen in Figure 4, apart from their type, cranes can be defined by their location in cargo movement operations. For example, STS cranes, the ones nominally used to move goods ship to shore, or visa-versa, must be large enough service the ships berthed at the terminal. This can be seen on the left of Figure 4. On the right, the authors primarily see cranes used to load goods onto trucks and rail to be distributed in-land. It is important to note, however, that not all cargo flow left to right, or right to left, as cargo can be re-routed to other ships for international waters, river, or even coastal transport. Many of the cranes servicing STS or to inland are be relatively fixed, either completely or to limited railing; however, in the centre of Figure 4's, operational flows smaller mobile cranes, such as rubber tyre gantry cranes, are more common. These provide critical mobile services and tend to be smaller to provide these services better. While there are many types of cranes, as some can be fairly specialised, this section is classifying them as limited movement, and those that are fully mobile.

Mobile cranes and those that have limited movement, consigned to a small designated area at a terminal, present two different cyber-physical risk profiles. This primarily rests on the types of wireless control and access they are likely to have. Mobile cranes will require more technology and solutions relating to driving and navigation. In comparison, nominally stationary cranes require more technology and solutions to service a wide number of mobile vehicles, of different sizes. This can be particularly tricky with ships, which may pitch or shift depending on how calm the winds and waters are. While there are several attack vectors, as discussed in detail below in Section 3.3.2, the focus of this paper, and the scenario used, is wireless attacks affecting cargo movement. This is key, as sensors and wireless solutions enabling remote control/access and autonomous operations are growing in both next-generation smart ports and industry (Macron, et al., 2019), which have similar concerns. Therefore, more specifically, the authors are interested in examining cyber-physical risks of Wi-Fi, radio, satellite (e.g. 3G/4G/5G) and both local and remote networks.

3.3.2. Possible Attack Vectors

Unlike the power infrastructure scenario, much of the wireless technology and vulnerabilities discussed in Section 2.2 are similar to how they are used in other sectors. Therefore, most vulnerabilities covered in the previous section would, in many instances, be equally applicable here. This section instead focuses on using these technologies in the context of a port, and in the second Cyber-MAR scenario specifically. Since Pilot$_2$ is focused on one system type (i.e. cranes) and one main outcome (i.e. delay), instead of looking at one attack chain and looking at the change of risk as an attack progresses in one port scenario, in this section, the authors shall examine different terminal setups, all deviations from the port examined for the project, in terms of crane technologies, layout, and numbers. With this, it became possible to generalise the risks subsequently in Section 4 further. In particular, it becomes easier to examine future concerns with continuing trends of IT/OT convergence and increasing remote control and autonomous/semi-autonomous operations. Possible attack vectors include those in remote driving for mobile cranes, and both remote access and autonomous control of stationary cranes designed to increase efficiency. Alternatively, wireless communications can also be used to access remote monitoring, using wireless sensor networks (WSNs) (Aalsalem, Khan, Gharibi, Khan, & Arshad, 2018), and attacking those can affect the accuracy, trustworthiness, and authenticity of the information. While this might not directly cause delays, this could confuse further down the operation chain and cause delays as a secondary effect.

3.3.3. Outcomes

As discussed previously in Section 2.2, while the vulnerabilities of wireless technologies are well researched, the outcomes differ significantly due to the environment within which they are executed. For example, in a white paper concerning the possible outcomes of hacking robots, it is made clear that the cyber-physical consequences of hacking such robots are highly dependent on context (Cerrudo & Apa, 2017). This article explains how robotics are one of the most dangerous scenario contexts, as robotic and mechanical systems are usually larger, more powerful, and programmed for fine-grained movements. This makes them capable of inflict damage on a large scale as well.

The financial risks are also higher, both in terms of damage to the robots themselves, physical damage they can cause, and operational delays. Lastly, the paper points out that industrial settings are dangerous as there are often several robots with the same configurations and/or residing on the same networks, making them easier for an attacker to hack multiple systems (e.g., shared passwords, similar software vulnerabilities). Assuming that (Cerrudo & Apa, 2017) considered transport industries, including maritime, in their assessment of robots in industry, all these issues are prevalent in the maritime sector, and in the pilot scenarios examined during this project.

Cranes exemplify these issues, as they are exceptionally large compared to other machinery used in other industries, with the larger stationary ones often over 100 feet (30 meters). Most cranes will also have multiple degrees of motion to move cargo (PEMA, 2016), and all of these motions are realised with robotic mechanics and have lifting capabilities on the order of tonnes. Furthermore, a port terminal often has multiple cranes of the same type and lined up to provide similar or identical services. The security concerns that more IoT and converging IT/OT means more robotic mechanisms will be integrated with monitoring systems to enable the remote control of wireless systems (Quarta, et al., 2017). There are many other reasons why cranes may be outfitted with sensors, as crane infrastructure receive much structural stress, and to prevent cracks or snapped wires sensors systems like those used on bridges and other structure sensors that can be used to monitor structural integrity and performance (Sumitro, Jarosevic, & Wang, 2002). Sensors for weight loads can also be used, as overloading and falling loads are some of the most common crane hazards in a port (Ren, Skjetne, & Gao, 2019). This monitoring information can be fed into critical decision making. Therefore altering this data could cause issues downstream. As a part of crane hazards, human error is another big factor, which has increased the need for both human error identification and corresponding autonomous solutions (Mandal, et al., 2015). This extends wireless communications past monitoring to a more bi-directional flow of information and commands. This dramatically increases the cyber-physical risks if an attacker can successfully hijack a crane. While the focus of Pilot$_2$ is on cranes, other services at ports (e.g. oil and gas) may also face similar cyber-physical risks in the future (Aalsalem, Khan, Gharibi, Khan, & Arshad, 2018).

As explained previously, a terminal often has multiple cranes lined up, sometimes several servicing the same large container ship. While there are no noticeable hacking examples out there, it is possible to examine the outcomes of other accidents to understand the potential outcomes. In one example, a crane collapsed onto a cargo ship in Vancouver, reducing throughput in that terminal for eight days (CBS, 2019). This is an interesting hypothetical cyber-physical example, because if it were to occur, not only was the damaged crane reducing port throughput but since the ship was trapped next to the terminal the other cranes blocked by the ship were unable to service other ships, compounding the reduction in operations. Hypothetically, another cyber-physical example of how a crane can affect operations is the cascading effect on the supply of the goods chain as it reduces a port capacity to move goods between different modes of transport. Understanding these wider effects are critical and will be considered as a part of Cyber-MAR and another research projects but unfortunately are outside the scope of this paper. However, looking down the supply chain outside port operations, it is important to note that trains, ships, and trucks are seeing similar evolutions in technology. Some of these networks are even designed to help load/offload cargo at the port by integrating seamlessly into port IT systems. Ship sensors and crane technologies are beginning to increase collaboration, for example, to increase efficiency by reducing ship movement issues like load pendulation and ship pitching or rolling (McKenzie, 2020). This poses a potential threat vector between port cranes and other vehicles or vessels, and misinformation may increase risks.

4. Maritime Cyber Risk Assessment (MaCRA)

Regulations for maritime-cyber risk assessment in the sector is relatively new (IMO, 2020) and documents from several nations have highlighted the lack of cybersecurity in maritime risk assessments over the last few years (Wilshusen, 2015). Paraphrasing from previous works (Polemi, Ntouskas, Theoharidou, & Gritzalis, 2013) (Tam & Jones, 2019c) the static nature of most risk assessment models (e.g. NIST, FMEA, CRAMM, OCTAVE) are insufficient to provide an accurate picture as maritime transport are dynamic systems, with cyber and cyber-physical parameters that greatly affect risks. Most also fail to examine the cyber-physical aspect, as unique, physical, actions that can be triggered by cyber events or visa-versa.

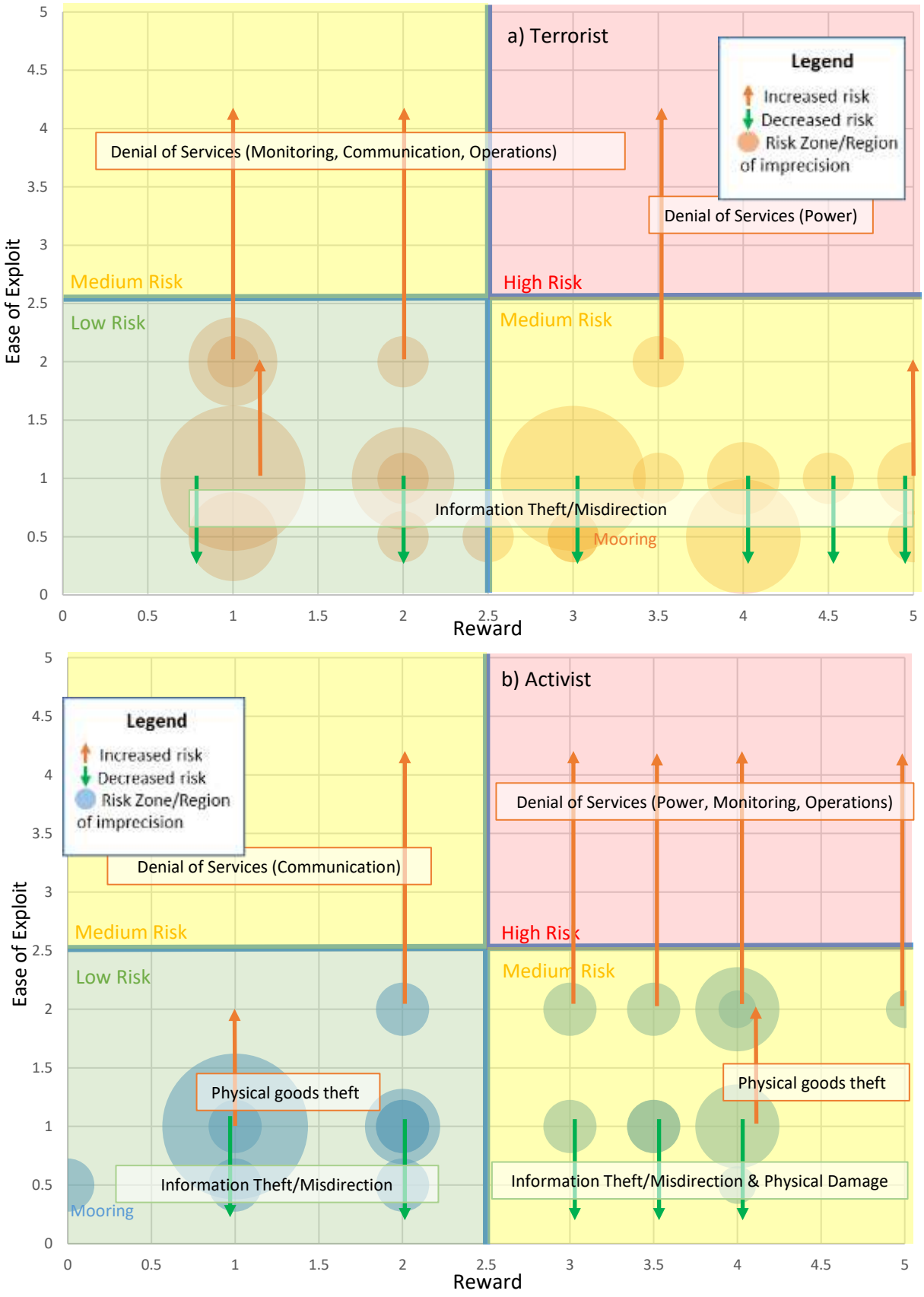
Research surrounding the MaCRA framework has attempted to address this issue, specifically for cyber-maritime risks (Tam & Jones, 2019b). As a multi-dimensional model, it can consider static, dynamic, cyber, and physical elements that affect a set of maritime systems. While the initial paper was used to analyse several potential ship targets, as they were identified as the likely 'weak-link' in the maritime supply chain, this paper uses the MaCRA framework on port systems for the two pilot studies discussed. For the paper, 57 combinations of key port systems and possible outcomes (e.g. denial-of-service, damage, theft, misdirect) were identified in the same manner that ship bridge systems were in the original paper. However, when creating figures below, systems and outcomes were more likely to be selected if relevant to the scenarios looked at in the pilot studies, i.e. power outage and crane hijacking. This reduced the complexity of the figures, and to make assessments, even more, reader-friendly, risks were also combined into general risk zones (see original paper). Data labels for zones were also reduced or removed in Figures 5-6.

As a highly detailed model, MaCRA is designed to filter and project the relevant risk information to answer a question posted by an analyst. Unfortunately examining the issue of a power outage across an entire port does is still considerably complex, based on the background research into past events. Therefore, for the $Pilot_1$ power outage scenario, the model will also be excluding several attacker types, assessing only activists and terrorists as these groups are most likely to attempt triggering a port power outage. While other attackers such as pranksters criminals may carry out this attack, with the multiple attack steps involved and the severity of the outcome, the authors would classify such an attack at this level terrorist even if the origin is not a known terrorist individual or organisation. Unfortunately, by nature, it is difficult to show dynamic changes in static figures. However, Figure 5 attempts to do this with the arrows layered onto the baseline assessment to show the attack chain outcome. This helps show what risk changes are caused, or not connected to, scenario events. It is important to note that an attack triggering a power-outage, including backup-power, like this, is highly unlikely, however for $Pilot_1$ maximally severe outcomes are demonstrated.

Denying back-up power, or preventing power re-routing, is a significant challenge as power infastructure are built with multiple redundancies, which is why power outage "ease-of-exploit" never reaches the max value. $Pilot_1$ shows a very polarising effect, where most denials of service attacks become very easy on systems powered by the main grid. The exceptions are systems than can be powered by generators, particularly RTG cranes, and those that can easily have power re-routed them. In comparison, many risks with misdirection and data theft outcomes were dramatically reduced, as access would be denied to both victims and attackers in a power outage. The exception is the risk of physical theft, which increases for both attackers, but not as significantly, as locks, CCT/monitoring and scheduling may be affected. Some systems like mooring may also not be affected, as power may not be a factor in operations. This aspect may also increase or decrease depending on if attackers are remote or local.

Conversely, the $Pilot_2$ targets a small subset of port systems, unlike a full power-outage. The focus is on crane control/monitoring systems that could potentially lead to loss of control. As there will be more systems filtered out, and only DoS and damage as 'Delay' outcomes, Figure 6 can examine crane risks in more detail. Instead of a more detailed comparison of each attacker type, like the comparison of terrorist and activist in Figure 5, since the risks across all attacker types in $Pilot_2$'s risk assessment were relatively similar, the authors instead decided to divide the conceptual port of the second pilot into two terminals. As terminals in a port can have different crane distributions and configurations, number and position of various cranes, if a cyber-risk was mostly associated with one type of crane, STS, for example, the risks could vary between terminals. This is explored in Figure 6. For the sake of an interesting exercise, STS and RTG cranes in $Pilot_2$ have local wireless access enabled. This could be because they were more recently purchased or recently re-fitted to suit port needs. Furthermore, in this scenario, rail-mounted gantry (RMGC) cranes have yet to have remote support added, with pilot two's terminals having 80% and 50% wireless cranes (see Figure 6).

Figure 5: MaCRA assessment of a conceptual port with base risk and Pilot$_1$ power-outage change

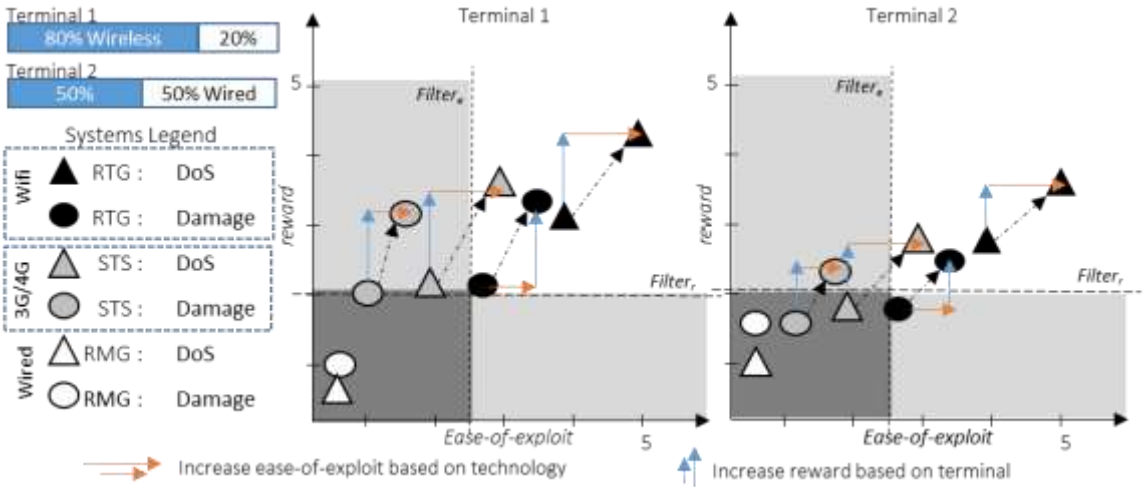


Source: authors own elaboration

Starting again from a base risk assessment, Figure 5 demonstrates the change in risk for both terminals based on a singular port event. While the base risk profile for individual terminals is shown, the overall port can be a summation or average of each point (see original paper for details). From Section 2, it is understood that multiple cranes can keep operations running despite singular accidents, however, if multiple cranes have similar cyber vulnerabilities and share the same network, the risk of a cyber-attack is much higher than an accident because of shared, if not identical, vulnerabilities..

As can be seen in Figure 6, the non-wireless cranes are the only systems unaffected by the port being exposed to a wireless attack designed to delay operations. That said, while the ease-of-exploit stays the same across the port, because of lack of wireless vulnerabilities, the reward of attacking these systems is slightly higher in Terminal 2 as there are more of these. As the main interest of Pilot$_2$ examined supply chain effects, Figure 6 looks at the 'delays' caused by denial of service and damage. Hijacking or misdirection can also be examined. From this, the terminal with more wireless connected cranes is at a higher risk of DoS, as encryption would protect the data itself. Please note axis orientation in Figure 6 match the original MaCRA paper, while those in Figure 5 were reversed to highlight risk increase and decrease. Unlike Figure 5, during a wireless attack, there are increased movements across both ease and reward axis triggered dynamically by a wireless attack being executed. In Pilot$_2$, these risk increases are attributed to how much easier it becomes to cause delays once an attack is underway, and the reward based on the terminal being attacked.

Figure 6 Macra risk assessment of cranes conceptual port with two terminals



Source: authors own elaboration

In terminals 1 and 2 smaller increases in risk happen with 3G/4G in contrast to Wifi, as public port networks are often vulnerable and satellite signal strength at ports is often not an issue. Conversely, the increase in reward in terminal 1 is greater than those in terminal 2 due to the number of potential targets (i.e. wireless cranes) available. This is worth considering when analysing supply chain econometric outcomes to a potential cyber-attack, as some terminals may service a different type or number of ships. Terminals can also be specialised to passenger or other types of cargo. However, as Pilot$_2$ is restricted to cranes, and therefore a container specialised port, the cyber risks of the two terminals are not so divergent. That said, one may be more well suited for the largest container ships, shorter routes, or a terminal may have more direct access to train terminals than others. While calculating the different econometric risks resulting from a delay is outside the scope of this paper, the purpose of using the MaCRA risk assessment framework in the Cyber-MAR project is to be able to create fine-grained cyber-risk assessments that can be passed to econometric and supply chain models to determine, with detail, what delays and risks that may result as effects ripple outward. Section 5 will further examine these observations and discuss future work in this area.

5. DISCUSSION

As a critical hub for transport, ports are important infrastructure that need to be cyber and cyber-physical secure especially, as more technological solutions are widely adopted to meet efficiency, ISPS code, ISM code, and environmentally friendly demands. Attacks have recently begun affecting maritime operations, at sea and at the port, and the history of other critical national infrastructure (e.g. power, oil) show how risks can continue to develop significantly in the maritime sector. As a part of an EU Project called Cyber-MAR, the authors have been given information from several ports regarding some of their systems and the environment they operate in. With Sections 3 and 4, this paper generalised the information provided to create conceptual cyber risk assessment to raise awareness without revealing real port vulnerabilities. Attack chains for each port pilot were derived from existing attacks on similar systems but adjusted for the maritime context to both demonstrate how realistic these scenarios could be, again without revealing real port vulnerabilities. With these conceptual risk profiles, the following subsections will discuss how they will be used in future Cyber-MAR work, and how these could be used to assess risks in a future smart port context which is not in the scope of this particular project.

5.1. Cyber-MAR

With the attack chains that fit both $Pilot_1$ and $Pilot_2$, the authors were able to create MaCRA models, with several projected views demonstrated in Figures 5-6. With a more detailed vulnerability analysis of specific port system and system components, these models can become highly detailed with several interesting risk assessment projections. The model, which is more high level, can also contextualise specific Cyber-MAR training scenarios derived from the pilots above. Further down the work stream, risk profiles will also be used to create econometric models, as mentioned several times, in order to quantify both the hours of delay and the financial cost of a cyber-attack in addition in addition to the risks. Factors such as cargo types and the use of trains or vehicles for distribution will affect the research as a follow up to the risk research demonstrated here. Highlighting top risks will also support why solutions such as network-based intrusion detection systems (IDS) are critical for mitigating a number or port risks (Khraisat, Gondal, Vamplew, & Kamruzzaman, 2019). For example, the Ukraine report did demonstrate how the attack on power supply infrastructure had a unique network signature that could be used to detect the attack in the future (Lee, Assante, & Conway, 2016). If MaCRA could be used to demonstrate the reduction in risk when a suitable maritime-cyber IDS is deployed on port networks, the benefits would be more clearly communicated. This can be combined with research into the robustness of power grids globally, or even specific to European grids given the scope of the Cyber-MAR project (Sole, Rosas-Casals, & Valverde, 2008).

It is also important to note that not all risks can be best solved by technical solutions like IDS, and that human training to reduce human error and as a check and balance for systems are important. Therefore, it is the goal of Cyber-MAR not only to create cyber-range training to train cyber-security specialists in IDS and other detection methods but also create training for mariners to empower them against cyber-attacks and to improve human-based mitigation strategies as well.

5.2. Smart ports

These two pilots, which deal with denial of service to power and delays cause to supply chain through wireless crane hijacking, while entirely appropriate to the project, is somewhat narrow in terms of possible cyber-attack objectives, outcomes, and severity. Looking at the future, as systems become more fine-tunes and increasingly complex, misinformation becomes a higher risk with this level of integration. For example, instead of completely shutting off power, misinformation could have more

subtle changes, such as lowering power output by falsely reporting that a transformer or other component are malfunctioning. As ports become more intelligent (i.e. Ports 4.0), either semi-autonomous or autonomous, certain types of risks are likely to increase faster, in terms of outcomes and severity, than others. This can be seen in next-generation industry solutions as well (i.e. Industry 4.0) where more intelligent anomaly detection is needed as the industrial robots themselves become more intelligent (Narayanan & Bobba, 2018). It is also important to note that the two pilots were based in ports specialised in container operations, and very similar Mediterranean regions.

Smart ports around the world will grow to suit more port services (e.g., oil, passenger) and research outside the project should not be limited to the locations and specialities of this project. Hazardous goods, lives, extreme weather, and political environments are all significant risk factors that were not explored in this paper but should be in future smart port research, when applicable. While there are many methods of big data analysis from other sectors that can be used to assess and analyse the cyber risks of a smart port, currently there is an issue of maritime systems, ports and ships, generating enough data that is useful for these types of analyses. Currently most systems generate and store information on physical elements. However, it is difficult to assess the cyber and cyber-physical risks with only physical-related data. Therefore, it is important to both begin collecting cyber-related information to feed into big data analysis (Boudehenn, Cexus, & Boudra, 2020) (Tam & Jones, 2019a), and create the technology to do so if it does not currently exist (Tam, Forshaw, Jones, 2019c). Future work may also include examining legal frameworks, such as the ISPS and ISM codes, to determine how well they reduce risks across IT and OT, or if there are biases to certain technologies or industries within the maritime sector.

6. CONCLUSIONS

Using knowledge gathered from partners as a part of the Cyber-MAR project and existing example of cyber vulnerabilities and attacks in similar infrastructure, this paper devised two attack scenarios that aligned with the two pilots of the project. This explored the possible outcomes resulting from an attack that targeted port power, and a wireless attack that targeted cranes and caused delays down the supply chain. Conceptualising these scenarios, and providing risk assessments of the two scenarios, this paper was able to demonstrate the dynamic changes to both cyber and cyber-physical risks at a port. From this, further work can be done to assess specific ports privately, to protect real port vulnerabilities, and create appropriate technical (IDS) and training solutions to mitigate the risks. These preliminary models also demonstrate how complex risks can become as ports become more technologically advanced, with the paper's conceptual findings identifying some elements that may become more relevant as ports continue to evolve in order to meet global demands.

ACKNOWLEDGMENTS

This paper is a part of the research efforts under Cyber-MAR. Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. The content reflects only the authors' view, and the European Commission is not responsible for any use that may be made of the information it contains.

AUTHOR BIOS

Professor Kevin Jones is the Executive Dean of Science and Engineering at the University of Plymouth, and the head of the Cyber-SHIP lab. He is also the principle investigator for University of Plymouth in several other projects including Cyber-MAR. Prior to joining Plymouth, he was Head of Computer Science at City University London and had previously spent a number of years in the

Silicon Valley. His research and teaching interests cover the Trustworthiness of Complex Systems, including Cyber Security, with a focus on the Maritime domain. Kevin is a Fellow of the IMARest, IET and the BCS, and a Liveryman of the WCIT.

Dr Kimberly Tam is a lecturer at the University of Plymouth, UK. Bridging the gap between the university's maritime navigation department and cyber-security research groups, she has been researching maritime cyber-security in depth since 2016. During those years she has published several papers, helped start a new maritime-cyber symposium to bring academia and industry together, and started several cyber-risk and cyber-vulnerabilities projects. She is also a co-investigator for the Cyber-MAR project, academic lead for the Cyber-SHIP project, and heavily involved other maritime cybersecurity projects.

Dr Kemedi Moara-Nkwe is a Research Fellow in Cyber Security at the University of Plymouth working on the Cyber-MAR project. Prior to joining Plymouth, he was a research associate in Computer Networking at Liverpool John Moores University working on the Liverpool 5G Deployment project. His research interests are in Cyber Security, Networking and Communications with applications in Maritime.

References

Aalsalem, M., Khan, W. Z., Gharibi, W., Khan, M. K., & Arshad, Q. (2018). Wireless Sensor Networks in oil and gas industry: Recent advances, taxonomy, requirements, and open challenges. *Network and Computer Applications*.

Adoghe, A., Awosope, C., & Ekeh, J. (2012). Asset maintenance planning in electric power distribution network using statistical analysis of outage data. *Electrical Power and Energy Systems.*

Akbar, A., Aasen, A., Msakni, M., Fagerholt, K., Lindstad, E., & Meisel, F. (2020). An economic analysis of introducing autonomous ships in a short-sea liner shipping network. *International Transactions in Operational Research.*

Allianz. (2014). *Lock & Dock Gates: Guidance on types, operating factors, failures and maintenance.* (Accessed 2020).

Antonio, Luque, A., Harrison, I., Pietrosanti, Stefano, Alasali, F., . . . Becerra, V. (2016). Energy reduction on eRTG. *Environment and Electrical Engineering.*

BBC. (2011). *Hackers 'hit' US water treatment systems.*

Belfast Harbour. (2019). *A Port for Everyone A Vision to 2035.*

Bi, W., Zhang, K., Wang, Y., & Ding, Z. (2019). Frequency Vulnerability Analysis of Power Systems Considering UAV Striking. *Asia-Pacific Power and Energy Engineering Conference (APPEEC).*

Bo, L., & Wang, L. (2019). Handling optimization Framework for Railway Container Terminal based on Vehicle Interconnection. *Journal of Physics.*

Boudehenn, C., Cexus, J.-C., & Boudra, A. (2020). A Data Extraction Method for Anomaly Detection in Naval Systems. *Cyber Science.* IEEE.

Brandy, D. (2018). *IoT in Maritime – Inmarsat Research Programme.* Digital Ship: SVP Market Strategy, Inmarsat Maritime.

Brogaonkar, R., Hirschi, L., Park, S., & Shaik, A. (2019). New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. *Privacy Enhancing Technologies.*

Brown, R. (2017). *Electric Power Distribution Reliability.* CRC Press.

CBS. (2019, Feb). *Collapsed crane removed from Port of Vancouver after 8-day operation*. Retrieved from https://www.cbc.ca/news/canada/british-columbia/crane-collapse-port-of-vancouver-1.5007680

Cerrudo, C., & Apa, L. (2017). *Hacking Robots Before Skynet.* IOActive.

Chen, T., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*.

Crouigneau, S., Bourdon, L., Billard, Y., Person, J., & Schoefs, F. (2008). Risk analysis to support operation and maintenance of an ageing dock-gate for the Port of Marseille Authority. *Applications Heritage and Constructions in Coastal and Marine Environment.*

Dai, L., Hu, H. W., & Wang, Z. (2020). Is Shore Side Electricity greener? An environmental analysis and policy implications. *Energy Policy*.

DNV GL. (2015). Ship connectivity . *Strategic Research & Innovation Position Paper.*

Duin, J., Geerlings, H., Tavasszy, L., & Bank, D. (2019). Factors causing peak energy consumption of reefers at container terminals. *Journal of Shipping and Trade.*

Edris, A., & Hoidalen, H. (2012). Medium frequency high power transformers, state of art and challenges. *Renewable Energy Research and Applications (ICRERA).*

ENISA. (2019). *Port Cybersecurity.*

Europa. (2020). *Maritime ports freight and passenger statistics: Statistics Explained.*

FCH. (2017). *Development of Business Cases for Fuel Cells and Hydrogen Applications for Regions and Cities.* Brussels.

Foster, J., Graham, W., Hermann, R., Kluepfel, H., Lawson, R., Soper, G., . . . Woodard, J. (2008). Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *Business & Economics*.

International Chamber of Shipping. (2019). Review of Maritime Transport. *International Chamber of Shipping, United Nations Conference on Trade and Development (UNCTAD).*

Jain, R., Chaudhary, D. K., & Kumar, S. (2018). Analysis of Vulnerabilities in Radio Frequency Identification (RFID) Systems. *Cloud Computing, Data Science & Engineering.* IEEE.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity.*

Khurana, H., Hadley, M., Lu, N., & Fincke, D. (2010). Smart-grid security issues. *IEEE Security & Privacy.*

Klinger, C., Landeg, O., & Murray, V. (2014). Power Outages, Extreme Events and Health: a Systematic Review of the Literature from 2011-2012. *Public Library of Science*.

Kosmowski, K., & Gotebiewski, D. (2019). Functional safety and cyber security analysis for life cycle management of industrial control systems in hazardous plants and oil port critical infrastructure including insurance. *Journal of Polish Safety and Reliability Association.*

Lasi, H., Fettke, P., Kember, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, (pp. pages239–242).

Lee, R., Assante, M., & Conway, T. (2016). *TLP: White. Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case.* SANS E-ISAC.

Macron, P., Arm, J., Benesi, T., Zezulka, F., Diedrich, C., Schroder, T., . . . Bradac, Z. (2019). New Approaches to Implementing the SmartJacket into Industry 4.0. *Sensors*.

Maersk. (2017, August). *A. P. Moller Maersk improves underlying profit and grows revenue in first half of the year*. Retrieved from https://edit.maersk.com/en/the-maersk-group/press-room/press-release-archive/2017/8/a-p-moller-maersk-interim-report-q2-2017

Man, Y., Lundh, M., & MacKinnon, S. (2018). *Managing unruly technologies in the engine control room: from problem patching to an architectural thinking and standardization.* WMU Journal of Maritime Affairs.

Mandal, S., Singh, K., Behera, R., Sahu, S., Raj, N., & Maiti, J. (2015). Human error identification and risk prioritization in overhead crane operations using HTA, SHERPA and fuzzy VIKOR method. *Expert Systems with Applications.*

Martin-Soberon, A., Monfort, A., Sapina, R., Monterde, N., & Calduch, D. (n.d.). Automation in port container terminals. *Social and Behavioral Science*, (p. 2014).

McKenzie, R. (2020). *Motion Compensation and Robotic Control of Maritime Cranes.* Carleton University Ottawa, Ontario.

Narayanan, V., & Bobba, R. (2018). Learning Based Anomaly Detection for Industrial Arm Applications. *Cyber-Physical Systems Security and Privacy.*

O'Flaherty, K. (2020). *U.S. Government Issues Powerful Cyberattack Warning As Gas Pipeline Forced Into Two Day Shut Down.* Forbes.

PEMA. (2016). *Practical Structural Examination of Container Handling Cranes in Ports and Terminals.*

Peng, Y., Li, X., Wang, W., Wei, Z., Bing, X., & Song, X. (2019). A method for determining the allocation strategy of on-shore power supply from a green container terminal perspective. *Ocean & Coastal Management*, (pp. 158-175).

Polemi, D., Ntouskas, T., Theoharidou, M., & Gritzalis, D. (2013). S-Port: Collaborative Security Management of Port Information Systems. *Conference: Information, Intelligence, Systems and Applications (IISA).*

Polemi, N. (2017). *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains.* Social Science.

PortForward. (2018). *Move Forward: Step by Step Towards A Digital Port.*

Quarta, D., Pogliani, M., Polino, M., Maggi, F., Zanchettin, A., & Zanero, S. (2017). An Experimental Security Analysis of an Industrial Robot Controller. *Symposium on Security and Privacy.* IEEE.

Ray, P. D., Harnoor, R., & Hentea, M. (2010). Smart power grid security: A unified risk management approach. *Carnahan Conference on Security Technology.*

Ren, Z., Skjetne, R., & Gao, Z. (2019). A Crane Overload Protection Controller for Blade Lifting Operation Based on Model Predictive Control. *Recent Advances in Offshore Wind Technology.*

Rockwell Collins. (2017). *The state of cybersecurity in the rail industry.*

Safa, H., Souran, D., Ghasempour, M., & Khazee, A. (2016). Cyber security of smart grid and SCADA systems, threats and risks. *CIRED Workshop.*

Simul8. (2020). Retrieved from https://www.simul8.com/

Sole, R., Rosas-Casals, M., & Valverde, S. (2008). Robustness of the European power grids under intentional attack. *Physical Review.* PubMed.

Sumitro, S., Jarosevic, A., & Wang, M. (2002). Elasto-magnetic sensor utilization on steel cable stress measurement. *Smart Mater Struct.*

Tam, K., & Jones, K. (2019a). Forensic Readiness within the Maritime Sector. IEEE Cyber SA, Oxford.

Tam, K., & Jones, K. (2019b). MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment. *WMU Journal of Maritime Affairs*.

Tam, K., & Jones, K. (2019c). Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector. International Journal on Cyber Situational Awareness.

Tam, K., Forshaw, K., & Jones, K. (2019). Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities. *International Conference on Marine Engineering and Technology.* OMAN.

Tam, K., Moara-Nkwe, K., & Jones, K. D. (2020). The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. *Maritime Technology and Research, 3(1), 16-30.*

Tan, S., De, D., Song, W.-Z., Yang, J., & Das, S. (2017). Survey of Security Advances in Smart Grid: A Data Driven Approach. *IEEE Communications Surveys & Tutorials.*

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., . . . Bursztien, E. (2017). Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials. *Computer and Communications Security.*

Wilshusen, G. (2015). *Maritime critical infrastructure protection: DHS needs to enhance efforts to address port cybersecurity.* GAO-16-116T.

Yang, Y., Zhong, M., Yao, H., Yu, F., Fu, X., & Postolache, O. (2018). Internet of things for smart ports: Technologies and challenges. *IEEE Instrumentation & Measurement Magazine* .